Outline for March 8, 2006

Reading: text, §12.2–12.5

1. Greetings and felicitations!
   a. Puzzle of the day
2. Attacks
   a. Exhaustive search: password is 1-8 chars, say 96 possibles; it's about 7×10^{16}
   b. Inspired guessing: think of what people would like (see above)
   c. Random guessing: can't defend against it; bad login messages aid it
   d. Scavenging: passwords often typed where they might be recorded as login name, in other contexts, etc.
   e. Ask the user: very common with some public access services
3. Password aging
   a. Pick age so when password is guessed, it's no longer valid
   b. Implementation: track previous passwords vs. upper, lower time bounds
4. Ultimate in aging: One-Time Password
   a. Password is valid for only one use
   b. May work from list, or new password may be generated from old by a function
5. Challenge-response systems
   a. Computer issues challenge, user presents response to verify secret information known/item possessed
   b. Example operations: $f(x) = x+1$, random, string (for users without computers), time of day, computer sends $E(x)$, you answer $E(D(E(x))+1)$
   c. Note: password never sent on wire or network
6. Biometrics
   a. Depend on physical characteristics
   b. Examples: pattern of typing (remarkably effective), retinal scans, etc.
7. Location
   a. Bind user to some location detection device (human, GPS)
   b. Authenticate by location of the device